REMARKS/ARGUMENTS

The following remarks are largely repeated from the Response After Final Rejection filed August 15, 2011. However, additional remarks are presented herein beginning at the bottom of page 14 in rebuttal to certain comments presented in the Advisory Action of September 19, 2011.

Suspension of Action

This Response is being filed with a Request for Continued Examination (RCE), which includes a request for a three-month suspension of action under 37 C.F.R. § 1.103(c) (see M.P.E.P. § 709). Accordingly, the Examiner is requested not to act on this application before May 15, 2012.

Status of Claims

Claims 7-18 are pending in the present application, of which claims 7 and 15 are independent claims. Claims 1-6 were previously canceled.

Overview of the Office Action

Claims 7 and 15 have been rejected under 35 U.S.C. § 103(a) as obvious over U.S. 2003/0131258 ("Kadri") in view of U.S. 6,631,416 ("Bendinelli"). Claims 8-14 and 16-18 have been rejected as obvious over Kadri in view of Bendinelli and U.S. 2004/0028035 ("Read").

Summary of Subject Matter Disclosed in the Specification

The following descriptive details are based on the specification. They are provided only for the convenience of the Examiner as part of the discussion presented herein, and are not intended to argue limitations which are unclaimed.

Disclosed embodiments are directed to a system for communication between a first computer terminal 1 in a private IP network 7 and a second computer terminal 5 in a public IP

network. The system includes network boundary equipment 3, e.g., a gateway or firewall. (See ¶ 17 of the published application, U.S. 2007/0258470 A1).

Conventionally, a packet arriving from the public network can be forwarded within the private network only if a packet from the private network has previously created a route for it. (See ¶ 8). However, in the disclosed embodiments, a mediation system 2 in the private IP network 7 that is associated with the first computer terminal 1 makes a TCP/UDP/IP interface available to the second computer terminal 5 via a control server 4 in the public IP network. (See ¶ 18). In particular, the mediation system 2 connects to a dedicated service port of the control server 4 via a TCP channel.

The mediation system 2 sets up a communications tunnel 6 through the boundary equipment 3 to the control server 4 via the dedicated service port. (See ¶¶ 19 and 21). The mediation system 2 uses this connection to inform the control server 4 about its state and environment in the private network. (See ¶ 24). The control server 4 can then perform various operations on the mediation system 2 via the communications tunnel 6 established through the boundary equipment 3. (See ¶ 25). These operations include such things as opening ports on the mediation system 2 and relaying packets through the mediation system 2 to ports in the private network.

Descriptive Summary of the Prior Art

Kadri

Kadri purports to allow efficient communication across firewalls by providing an internal contact point located inside the firewall which is used as a contact point for the inside peers. The internal contact point establishes a continuous connection to the outside relay server through tunneling. (Kadri at ¶ 12).

Fig. 1 of Kadri depicts a system 100 which includes a firewall 110, a relay server 120, an external peer 130, and a network 140. Within the firewall 110 is a gateway device 150, an internal contact point 160, N registered internal peers 170_1 to 170_N, and K unregistered internal peers 180_1 to 180_K. The gateway device 150 is located at the firewall boundary between the protected internal network and the external world. (Kadri at ¶¶ 18-20).

The internal contact point 160 is the central contact point for the peers 170_1 to 170_N inside the firewall 110. The internal contact point 160 communicates with the gateway device 150 via a tunnel 165. Thus, the internal contact point 160 communicates to the relay server 120 or the external peer 130 via the gateway device 150, and forwards the information or messages received from the external peer 130 and other external peers to the registered internal peers. (Kadri at ¶ 26).

The internal peers 170_1 to 170_N register to the internal contact point 160 to appoint the internal contact point 160 to be their contact point for external communication with devices outside the firewall 110 such as the external peer 130. The internal peers 170_1 to 170_N may send messages to the outside world such as the external peer 130 directly via the gateway device 150 or via the internal contact point 160. The internal peers 170_1 to 170_N, however, receive the messages sent from external devices such as the external peer 130 from the internal contact point 160 only. (Kadri at ¶ 27).

The relay server 120 is a server that has a tunnel 155 to the gateway device 150. The relay server 120 may contain software to provide cross-firewall interaction. The relay server 120 has interfaces to a number of external peers 130 which seek to communicate with the internal peers 170_1 to 170_N. (Kadri at ¶ 29).

As depicted in Fig. 2 of Kadri, the gateway interface 210 interfaces internally to the gateway device 150 located at the firewall 110. According to Kadri, when required, the gateway interface 210 establishes a continuous connection to the relay server 120 outside the firewall 110 through tunneling. The gateway interface 210 is also responsible for forwarding the registration information of the registered internal peers 170_1 to 170_N to the relay server 120 such that the relay server 120 is notified that these internal peers are now represented by the internal contact point 160. (Kadri at ¶ 32).

Bendinelli

Bendinelli relates to setting up virtual private networks (VPNs) which are self-configured on nonproprietary hardware, such as a standard personal computer (PC), rather than requiring specialized hardware, in order to establish virtual private networks over a local or wide geographical area. (Bendinelli at col. 3, lns. 50-62). According to Bendinelli, a prospective user or customer may contact a mediation point or a control system, such as a network operations center via a base network and indicate a desire to establish one or more virtual private networks. After configuration is completed and based on the user's request, the network operations center may enable one or more virtual private networks between the gateway and other gateways configured through the network operations center. (Bendinelli at col. 11, lns. 19-23).

Fig. 6A of Bendinelli shows a network 600 which may include one or more local area networks (LANs) 660, 661, a first, second, and third gateways 650-652, the Internet 620 and/or Intranet access (not shown), and a network operations center 610. The network operations center 610 may determine a virtual address for each gateway desiring to participate in one or more virtual private networks established through a base network 620. The virtual address, which may be in an IP format, may be used by the gateways to establish one or more tunnels with each other

through a base network 620 and may be routable only through the established tunnels. Based on the virtual addresses determined by the network operations center 610 and provided to the gateways 650, 651, 652, one or more virtual private networks may be established over the network 620. (Bendinelli at col. 20, lns. 14-58).

Fig. 13 of Bendinelli depicts steps for establishing a tunnel between two gateways in the network 600 (see Fig. 6A) for the case in which a gateway seeks to establish a tunnel with another gateway that is behind a firewall and is not accessible because the firewall selectively restricts information flowing to the gateway. For example, after the first gateway 650 and the second gateway 651 have registered and established control paths with the network operations center 610, the first gateway 650 may seek to establish a tunnel to the second gateway 651. (Bendinelli at col. 36, line 61 – col. 37, line 11).

According to Bendinelli, if both the originating gateway (e.g., the first gateway 650) and the destination gateway (e.g., the second gateway 651) are behind firewalls (steps 1330 and 1390), a direct tunnel between the originating gateway and the destination gateway may not be possible because the firewall may hide the real or public IP addresses of the originating gateway and destination gateway, respectively. As a result, the network operations center 610 may enable at the proxy module 613 a proxy (referred to as a "Hairpin") (step 1391) to enable a tunnel between the first gateway and the second gateway 651 through the proxy. When the Hairpin is enabled, the originating gateway and the destination gateway may exchange information through the Hairpin, each bypassing the firewall of the other gateway (step 1392). (Bendinelli at col. 37, line 61 – col. 38, line 12; see also Fig. 15A, col. 38, line 59 – col. 40, line 50).

Patentability over the Prior Art

The disclosed invention, as discussed above, allows for incoming packets to reach devices in the private network without requiring the device in the private network to first send out a packet to open a route through the firewall. This can be useful in situations in which the device in the private network is unable to send out a packet to the public network device with which it is seeking to communicate (see pub. app. at ¶ 10).

To implement this functionality, the disclosed invention uses a mediation system 2 within the private network, which is connected to a control server 4 in the public network via a tunnel. Once the tunnel is established, certain information is sent from the mediation system 2 to the control server 4. Then, the control server 4 can perform certain functions on the mediation system, such as opening and redirecting ports. This allows the control server 4 to reach the devices within the private network through the mediation system, even though a route to the device within the private network has not been previously established through the firewall.

Independent claim 7 recites, *inter alia*: "transmitting information, by the mediation system, to the control server relating to the configuration of the mediation system in the private network;" and "performing an operation, by the control server, on the mediation system via the communications tunnel established through the network boundary equipment."

These features may be understood by referring, for example, to the specification at ¶¶ 24-28 of the published application:

> [0024] To be initialized, the mediation system 2 connects to a fixed port of the control server 4 via a TCP channel. It uses this connection to inform the server 4 about its state and about its environment. This information can range from a description of its configuration in the private network 7 (IP address, subnetwork mask, etc.), through authentication or identification, to a description of the service that it wishes to use.

> [0025] Once initialization has been effected, three types of operation are effected between the system 2 and the server 4:
>
> [0026] Requests: open, redirect, connect, make server, and close ports.
>
> [0027] Packet and event relay.
>
> [0028] Maintain channel.

The primary cited reference, Kadri, merely discloses a means for "relaying," i.e., passing, received information to registered devices within a private network using a relay server:

> [0033] The collector 220 collects messages sent by the outside world such as the external peer 130. The messages are intended for any one of the internal peers 170_1 to 170_N. The collector 220 may also collect messages sent by the internal peers 170_1 to 170_N when the internal peers 170_1 to 170_N want to send messages via the internal contact point 160 rather than directly to the gateway device 150.

(Kadri at ¶ 33; see also ¶¶ 34-36).

Kadri is silent as to the specifics of the interaction between the internal contact point 160 and gateway device 150 (which the Office Action identifies as corresponding to the claimed mediation system) and the relay server 120 (which the Office Action identifies as corresponding to the claimed control server). Thus, as the Office Action acknowledges at pages 4-6, Kadri does not teach or suggest "transmitting information, by the mediation system, to the control server relating to the configuration of the mediation system in the private network;" and "performing an operation, by the control server, on the mediation system via the communications tunnel established through the network boundary equipment," as recited in claim 7.

The Office Action cites Bendinelli as disclosing these claimed features missing from Kadri. However, as discussed in further detail below, Bendenelli does not remedy the shortcomings of Kadri with respect to the features of claim 7.

The Office Action cites col. 37, lines 1-11, of Bendinelli as disclosing the claimed step of "transmitting information, by the mediation system, to the control server relating to the configuration of the mediation system in the private network." However, this cited portion merely describes the establishment of a VPN between two nodes which have previously connected to a network operations center. The information exchanged between the nodes, e.g., virtual IP addresses and shared secrets (see cited col. 21, lines 30-38), is information necessary for establishing a VPN, rather than information "relating to the configuration of the mediation system in the private network." Indeed, Bendinelli discloses connecting nodes which are not even associated with a private network (see col. 20, lines 20-30).

The Office Action also cites col. 37, line 53 – col. 38, line 12; and col. 39, line 39 – col. 40, line 40 of Bendinelli as disclosing the claimed step of "performing an operation, by the control server, on the mediation system via the communications tunnel established through the network boundary equipment." However, these cited portions merely describe the establishment of a VPN between nodes which are located behind a firewall. This is done by having each of the nodes connect to a proxy node, because their firewalls will not allow the incoming traffic necessary for establishing the VPN.

The Office Action refers, in particular, to the ability of the network operations center to turn firewall rules off and on. However, the firewalls do not correspond to the claimed mediation system. Thus, there is no teaching or suggestion in these cited portions of a control server (which the Office Action identifies as corresponding to the network operations center) performing an operation on a mediation system (which the Office Action identifies as corresponding to the gateways).

Furthermore, in the Advisory Action dated September 19, 2011, the Examiner states:

> [A] proxy module, located at the network operations center, is operative to supply a tunnel through the firewalls of both first and second gateways in order to set a TCP connection. This is sufficient to show an "operation" being performed by a server.

(Advisory Action at pages 2-3).

However, claim 7 requires that the operation is performed "via the communications tunnel established through the network boundary equipment." In other words, the operation is performed after a tunnel is set up. Therefore, the setting up of a tunnel, in and of itself, cannot correspond to the claimed "operation," as the Examiner contends.

It is clear from the discussion above that Bendinelli does not remedy the shortcomings of Kadri with respect to "transmitting information, by the mediation system, to the control server relating to the configuration of the mediation system in the private network;" and "performing an operation, by the control server, on the mediation system via the communications tunnel established through the network boundary equipment," as recited in claim 7.

Regarding the combination of Kadri and Bendinelli hypothesized by the Examiner, Applicants note that "[t]he key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious." M.P.E.P. § 2142 (citing *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398, ___, 82 USPQ2d 1385, 1396 (2007)). The Examiner puts forth the following rationale for why one of ordinary skill in the art would have combined the teachings of Kadri and Bendinelli:

> It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the method of communicating between terminals as disclosed by Kadri to include control established by a terminal as disclosed by Bendinelli to connect a plurality of gateways in order to establish a virtual private network in the analogous field of firewall tunneling. This is beneficiary to the method in that unnecessary overhead in setting up virtual private networks is reduced (Bendinelli: Col. 3, lines 30-46).

(Office Action at page 5).

This rationale is deemed to be flawed for at least the following reasons.

Kadri is concerned with allowing devices outside a private network to communicate with devices inside the private network, e.g., to send an http connection request to a device in the private network. This is done using a relay server which is connected via a tunnel to an internal device of the private network. By this mechanism, packets from outside devices can purportedly reach devices in the private network even though a route has not been previously established through the firewall.

Bendinelli, on the other hand, is concerned with establishing virtual private networks (VPNs) between networks. A VPN provides continuous encrypted communication between networks, which is entirely different than the sending and receiving of unencrypted http connection requests from outside devices. The solution disclosed in Bendinelli is therefore more complex than that disclosed in Kadri.

Thus, one of ordinary skill in the art implementing the teachings of Kadri would have had no reason to turn to Bendinelli, because Bendinelli is solving an entirely different and more complex technical problem than Kadri. Moreover, the Examiner's assertion that Bendinelli discloses a system in which "unnecessary overhead in setting up virtual private networks is reduced" is not relevant, because a practitioner following the teachings of Kadri is not seeking to establish VPNs.

In view of the above, claim 7 is deemed to be patentable over the Examiner's proffered combination of Kadri and Bendinelli.

The other cited reference, Read, was cited as disclosing the features of certain dependent claims. However, nothing has been found in Read that would remedy the deficiencies of the combination of Kadri and Bendinelli with respect to the features of claim 7 discussed above.

Independent claim 15, recites features similar to claim 7 and is therefore also deemed to be patentable over the applied prior art for reasons discussed above with respect to claim 7.

Claims 8-14 and 16-18, which each depend from one of independent claims 7 or 15, distinguish the invention over the applied prior art for reasons discussed above in regard to the independent claims as well as on their own merits.

Conclusion

Based on all of the above, the present application is now in proper condition for allowance. Prompt and favorable action to this effect and early passing of this application to issue are respectfully solicited.

It is believed that no additional fees or charges are required at this time in connection with the present application. However, if any additional fees or charges are required at this time, they may be charged to our U.S. Patent and Trademark Office Deposit Account No. 50-3111.

Respectfully submitted,
COZEN O'CONNOR

By /Carl B. Wischhusen/
Carl B. Wischhusen
Reg. No. 43,279
277 Park Avenue
New York, New York 10172
(212) 883-4900

Dated: February 15, 2012

NYC_MIDTOWN\1931913\1 298949.000